Федеральное агентство по рыболовству
БГАРФ ФГБОУ ВО «КГТУ»
Калининградский морской рыбопромышленный колледж

Утверждаю
Заместитель начальника колледжа
по учебно-методической работе
А.И.Колесниченко

Подписано цифровой подписью: Колесниченко Андрей Игоревич
Причина: Я утвердил этот документ
Дата: 17 Март 2025 г. 13:04:41
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России, CN=Федеральное казначейство

МДК.07.02 Сертификация информационных систем

Методические указания для выполнения практических занятий
по специальности
09.02.07 Информационные системы и программирование

МО-09 02 07-МДК.07.02.ПЗ

РАЗРАБОТЧИКИ	Богатырева Т.Н.
ЗАВЕДУЮЩИЙ ОТДЕЛЕНИЕМ	Бакулин А.М.

ГОД РАЗРАБОТКИ	2022
ГОД ОБНОВЛЕНИЯ	2025

Содержание

Практическая работа 1. Резервное копирование: цели, методы, концепции, планирование, роль журнала транзакций. Виды резервных копий

Резервное копирование: назначение, виды

Резервное копирование (англ. backup copy) — процесс создания копии данных на носителе (жёстком диске и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Цель:

Резервное копирование необходимо для возможности быстрого и недорогого восстановления информации (документов, программ, настроек и т. д.) в случае утери рабочей копии информации по какой-либо причине. Кроме этого, решается проблема передачи данных и работы с общими документами.

Требования к системе резервного копирования:

1. Надёжность хранения информации — обеспечивается применением отказоустойчивого оборудования систем хранения, дублированием информации и заменой утерянной копии другой в случае уничтожения одной из копий (в том числе как часть отказоустойчивости).

2. Многоплатформенность - полноценное функционирование системы резервного копирования в гетерогенной сети (гетерогенная компьютерная сеть — вычислительная сеть, соединяющая персональные компьютеры и другие устройства с различными операционными системами или протоколами передачи данных) предполагает, что её серверная часть будет работать в различных операционных средах и поддерживать клиентов на самых разных аппаратно-программных платформах.

3. Простота в эксплуатации — автоматизация (по возможности минимизировать участие человека: как пользователя, так и администратора).

4. Быстрое внедрение — простая установка и настройка программ, быстрое обучение пользователей.

Ключевыми параметрами резервного копирования являются:

- RPO — Recovery Point Objective;

- RTO — Recovery Time Objective.

RPO определяет точку отката — момент времени в прошлом, на который будут восстановлены данные, а RTO определяет время, необходимое для восстановления из резервной копии.

Виды резервного копирования

Существует несколько видов резервного копирования:

1. Полное резервное копирование (Full backup)

Полное копирование обычно затрагивает всю систему и все файлы. Еженедельное, ежемесячное и ежеквартальное резервное копирование подразумевает создание полной копии всех данных. Обычно оно выполняется тогда, когда копирование большого объёма данных не влияет на работу организации. Для предотвращения

большого объёма использованных ресурсов используют алгоритмы сжатия, а также сочетание этого вида с другими: дифференциальным или инкрементным. Полное резервное копирование незаменимо в случае, когда нужно подготовить резервную копию для быстрого восстановления системы с нуля.

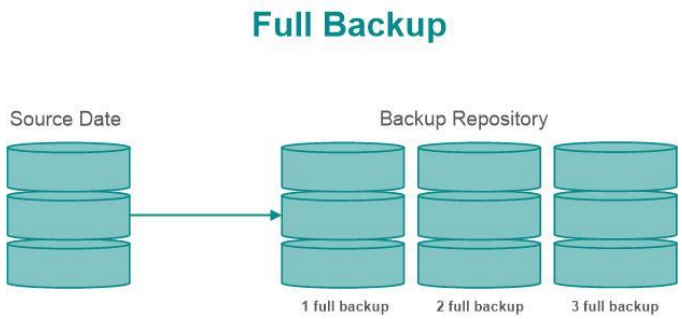
Обычно, полные резервные копии делают периодически и объединяют их с другими типами резервного копирования.

Преимущества Full Backup:

- быстрое восстановление данных
- простое управление
- все данные содержаться в одной резервной копии

Недостатки Full Backup:

- требует много места для хранения резервных копий
- высокая загрузка сети
- длительное выполнение резервного копирования



2. Дифференциальное резервное копирование (Differential backup)

При дифференциальном («разностном») резервном копировании каждый файл, который был изменён с момента последнего полного резервного копирования, копируется каждый раз заново. Дифференциальное копирование ускоряет процесс восстановления. Все копии файлов делаются в определённые моменты времени, что, например, важно при заражении вирусами.

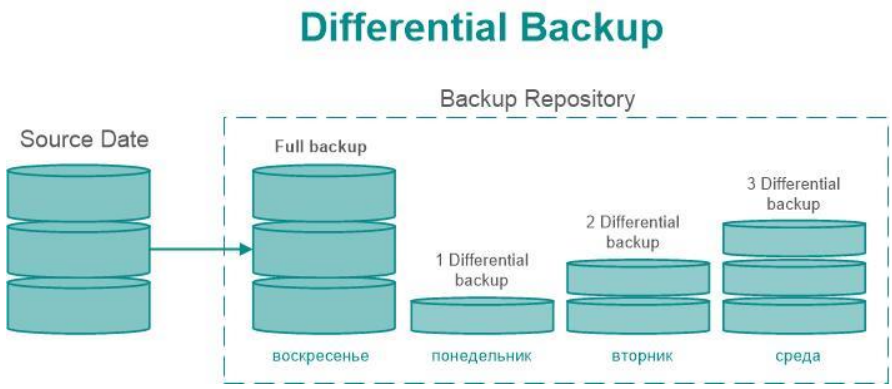
Дифференциальная резервная копия позволяет быстрее восстанавливать данные по сравнению с инкрементным резервным копированием, поскольку для этого требуется всего две части резервной копии: полная резервная копия и последняя дифференциальная резервная копия. Скорость резервного копирования / восстановления, находится где-то между полным и инкрементным методом резервного копирования. Резервное копирование выполняется быстрее, чем полная резервная копия, но медленнее, чем инкрементное резервное копирование. Восстановление выполняется медленнее, чем у полной резервной копии, но быстрее, чем у инкрементных резервных копий. Объем памяти, необходимый для дифференциального резервного копирования, по крайней мере на определенный период меньше, чем требуется для полного резервного копирования и больше, чем требуется для инкрементного резервного копирования.

Преимущества Differential Backup:

- резервное копирование быстрее, чем полное, но медленнее, чем инкрементное
- восстановление быстрее, чем инкрементное, но медленнее чем полное
- более надежный способ (для восстановления требуется только полная и последняя резервная копия)

Недостатки Differential Backup:

- каждый последующий бэкап выполняется дольше по времени и занимает больше дискового пространства в хранилище



3. Инкрементное резервное копирование (Incremental backup)

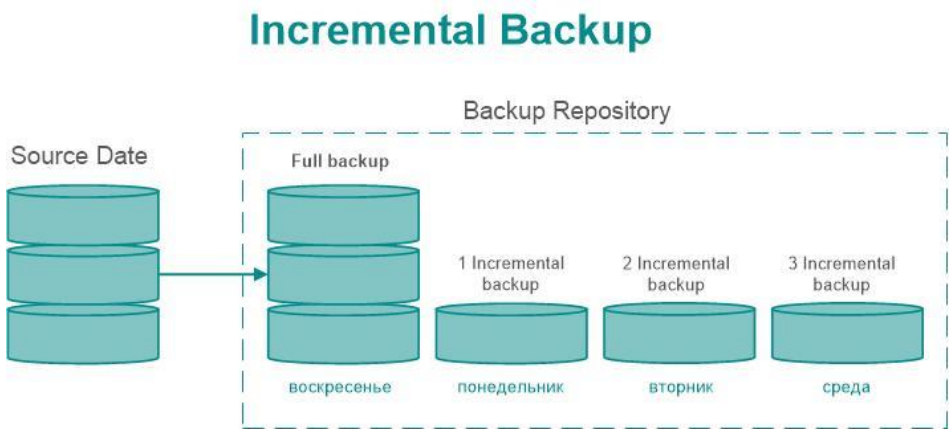
При добавочном («инкрементном») резервном копировании происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование. Последующее инкрементное резервное копирование добавляет только файлы, которые были изменены с момента предыдущего. Инкрементное резервное копирование занимает меньше времени, так как копируется меньшее количество файлов. Однако процесс восстановления данных занимает больше времени, так как должны быть восстановлены данные последнего полного резервного копирования, а также данные всех последующих инкрементных резервных копирований. В отличие от дифференциального копирования, изменившиеся или новые файлы не замещают старые, а добавляются на носитель независимо.

Преимущества Incremental Backup:

- высокая скорость резервного копирования (копируются только блоки изменённых данных)
- меньше места для хранения (по сравнению с полным)
- большее количество точек восстановления

Недостатки Incremental Backup:

- низкая скорость восстановления данных (необходимо восстановить как начальную полную копию, так и все последующие блоки)
- менее надежна (зависит от целостности всех блоков в цепочке)



4. Клонирование

Клонирование позволяет скопировать целый раздел или носитель (устройство) со всеми файлами и каталогами в другой раздел или на другой носитель. Если раздел является загрузочным, то клонированный раздел тоже будет загрузочным.

5. Резервное копирование в виде образа

Образ — точная копия всего раздела или носителя (устройства), хранящаяся в одном файле.

6. Резервное копирование в режиме реального времени

Резервное копирование в реж име реального времени позволяет создавать копии файлов, каталогов и томов, не прерывая работу, без перезагрузки компьютера.

7. Холодное резервирование

При холодном резервировании база данных выключена или закрыта для потребителей. Файлы данных не изменяются и копия базы данных находится в согласованном состоянии при последующем включении.

8. Горячее резервирование

При горячем резервировании база данных включена и открыта для потребителей. Копия базы данных приводится в согласованное состояние путём автоматического приложения к ней журналов резервирования по окончании копирования файлов данных.

Задание.

Создайте презентацию по материалам лекции Резервное копирование

Практическая работа 2. Утилиты резервного копирования

Схемы ротации

Смена рабочего набора носителей в процессе копирования называется их ротацией. Для резервного копирования очень важным вопросом является выбор подходящей схемы ротации носителей (например, магнитных лент).

1. Одноразовое копирование

Простейшая схема, не предусматривающая ротации носителей. Все операции проводятся вручную. Перед копированием администратор задаёт время начала резервного копирования, перечисляет файловые системы или каталоги, которые нужно копировать. Эту информацию можно сохранить в базе данных, чтобы её можно было использовать снова. При одноразовом копировании чаще всего применяется полное копирование.

2. Простая ротация

Простая ротация подразумевает, что некий набор лент используется циклически. Например, цикл ротации может составлять неделю, тогда отдельный носитель выделяется для определённого рабочего дня недели. Недостаток данной схемы — она не очень подходит для ведения архива, поскольку количество носителей в архиве быстро увеличивается. Кроме того, инкрементальная/дифференциальная запись проводится на одни и те же носители, что ведёт к их значительному износу и, как следствие, увеличивает вероятность отказа.

3. «Дед, отец, сын»

Данная схема имеет иерархическую структуру и предполагает использование комплекта из трёх наборов носителей. Раз в неделю делается полная копия дисков компьютера («отец»), ежедневно же проводится инкрементальное (или дифференциальное) копирование («сын»). Дополнительно раз в месяц проводится ещё одно полное копирование («дед»). Состав ежедневного и еженедельного набора постоянен. Таким образом, по сравнению с простой ротацией в архиве содержатся только ежемесячные копии плюс последние еженедельные и ежедневные копии. Недостаток данной схемы состоит в том, что в архив попадают только данные, имевшиеся на конец месяца, а также в износе носителей.

4. «Ханойская башня»

Схема призвана устранить некоторые из недостатков схемы простой ротации и ротации «Дед, отец, сын». Схема построена на применении нескольких наборов носителей. Каждый набор предназначен для недельного копирования, как в схеме простой ротации, но без изъятия полных копий. Иными словами, отдельный набор включает носитель с полной недельной копией и носители с ежедневными инкрементальными (дифференциальными) копиями. Специфическая проблема схемы «ханойская башня» — её более высокая сложность, чем у других схем.

5. «10 наборов»

Данная схема рассчитана на десять наборов носителей. Период из сорока недель делится на десять циклов. В течение цикла за каждым набором закреплён один день недели. По прошествии четырёхнедельного цикла номер набора сдвигается на один день. Иными словами, если в первом цикле за понедельник отвечал набор номер 1, а за вторник — номер 2, то во втором цикле за понедельник отвечает набор номер 2, а за вторник — номер 3. Такая схема позволяет равномерно распределить нагрузку, а, следовательно, и износ между всеми носителями.

Схемы «Ханойская башня» и «10 наборов» используются нечасто, так как многие системы резервного копирования их не поддерживают.

Хранение резервной копии

- Лента стримера — запись резервных данных на магнитную ленту стримера;
- «Облачный» бэкап — запись резервных данных по «облачной» технологии через онлайн-службы специальных провайдеров;
- DVD или CD — запись резервных данных на компактные диски;
- HDD — запись резервных данных на жёсткий диск компьютера;
- LAN — запись резервных данных на любую машину внутри локальной сети;
- FTP — запись резервных данных на FTP-серверы;
- USB — запись резервных данных на любое USB-совместимое устройство (такое, как флэш-карта или внешний жёсткий диск).

Причины утери информации

Эксплуатационные поломки носителей информации

Описание: случайные поломки в пределах статистики отказов, связанные с неосторожностью или выработкой ресурса. Если важная информация уже потеряна, то можно обратиться в специализированную службу, но надёжность не стопроцентная.

Решение: хранить всю информацию (каждый файл) минимум в двух экземплярах (причём каждый экземпляр на своём носителе данных). Для этого применяются:

- RAID 1, обеспечивающий восстановление самой свежей информации. Файлы, расположенные на сервере с RAID, более защищены от поломок, чем хранящиеся на локальной машине;
- Ручное или автоматическое копирование на другой носитель. Для этого может использоваться система контроля версий, специализированная программа резервного копирования или подручные средства наподобие периодически запускаемого cmd-файла.

Стихийные и техногенные бедствия

Описание: шторм, землетрясение, кража, пожар, прорыв водопровода — всё это может привести к потере всех носителей данных, расположенных на определённой территории.

Борьба: единственный способ защиты от стихийных бедствий — держать часть резервных копий в другом помещении. В частности, помогает резервное копирование через сеть на компьютер, расположенный достаточно далеко (или в облачное хранилище данных).

Вредоносные программы

Описание: в эту категорию входит случайно занесённое ПО, которое намеренно портит информацию — вирусы, черви, «троянские кони». Иногда факт заражения обнаруживается, когда немалая часть информации искажена или уничтожена.

Борьба:

- Установка антивирусных программ на рабочие станции. Простейшие антивирусные меры — отключение автозагрузки, изоляция локальной сети от Интернета, и т. д.
- Обеспечение централизованного обновления: первая копия антивируса получает обновления прямо из Интернета, а другие копии настроены на папку, куда первая загружает обновления; также можно настроить прокси-сервер таким образом, чтобы обновления кэшировались (это всё меры для уменьшения трафика).
- Иметь копии в таком месте, до которого вирус не доберётся — выделенный сервер или съёмные носители.
- Если копирование идёт на сервер: обеспечить защиту сервера от вирусов (либо установить антивирус, либо использовать ОС, для которой вероятность заражения мала). Хранить версии достаточной давности, чтобы существовала копия, не контактировавшая с заражённым компьютером.
- Если копирование идёт на съёмные носители: часть носителей хранить (без дописывания на них) достаточно долго, чтобы существовала копия, не контактировавшая с заражённым компьютером.
- Использование носителей с однократной записью: CD-R, DVD-R, BD-R. Их объём недостаточен для серьёзных применений.

Человеческий фактор

Описание: намеренное или ненамеренное уничтожение важной информации — человеком, специально написанной вредоносной программой или сбойным ПО.

Борьба:

- Тщательно расставить права на все ресурсы, чтобы другие пользователи не могли модифицировать чужие файлы. Исключение делается для системного администратора, который должен обладать всеми правами на всё, чтобы быть способным исправить ошибки пользователей, программ и т. д.
- Построить работающую систему резервного копирования — систему, которой люди реально пользуются и которая достаточно устойчива к ошибкам оператора. Если пользователь не пользуется системой резервного копирования, вся ответственность за сохранность ложится на него.
- Хранить версии достаточной давности, чтобы при обнаружении испорченных данных файл можно было восстановить.
- Перед переустановкой ОС следует обязательно копировать всё содержимое раздела, на которой будет установлена ОС, на сервер, на другой раздел или на CD/DVD.
- Оперативно обновлять ПО, которое заподозрено в потере данных.

Затруднения при резервном копировании

Законы об авторском праве и других исключительных правах могут запрещать или ограничивать копирование. Иногда для резервного копирования предусматриваются исключения (см. Свободное использование произведений, ограничения и исключения в области авторского права).

Условия использования проприетарного программного обеспечения и других несвободных произведений также могут ограничивать или запрещать резервное копирование.

Технические меры защиты от копирования затрудняют резервное копирование независимо от законов и условий.

Задание

Создать интеллект-карту по теме Схемы ротации в программе xMind

Требования к интеллект-карте:

1. Карта должна раскрывать тему лекции полностью;

2. Должна быть отражена структура документа (главные разделы, подразделы, терминология, определения терминов (если таковые имеются в лекционном материале) и т.д.);

3. Не должно быть больших блоков текстового материала в одном разделе. Рекомендуется разбивать этот текст на несколько подразделов или конспективно сокращать;

4. Можно использовать иллюстрации в качестве разделов и подразделов;

5. Типом связи Отношения рекомендуется пользоваться в случаях, если раздел или понятие имеет отношение к нескольким разделам;

6. Карта не должна быть копией лекции.

Сохранить документ в программе xMind под своей фамилией и переслать преподавателю.

Практическая работа 3. Блокирование портов

Основные понятия Active Directory

Служба Active Directory

Расширяемая и масштабируемая служба каталогов Active Directory (Активный каталог) позволяет эффективно управлять сетевыми ресурсами.

Active Directory - это иерархически организованное хранилище данных об объектах сети, обеспечивающее удобные средства для поиска и использования этих данных. Компьютер, на котором работает Active Directory, называется ***контроллером домена***. С Active Directory связаны практически все административные задачи.

Технология Active Directory основана на стандартных Интернет – протоколах и помогает четко определять структуру сети.

Active Directory и DNS

В Active Directory используется доменная система имен.

Domen Name System, (DNS) — стандартная служба Интернета, организующая группы компьютеров в домены. Домены DNS имеют иерархическую структуру, которая составляет основу Интернета. Разные уровни этой иерархии идентифицируют компьютеры, домены организаций и домены верхнего уровня. DNS также служит для преобразования имен узлов, например zeta.webatwork.com, в численные IP-адреса, например 192.168.19.2. Средствами DNS иерархию доменов Active Directory можно вписать в пространство Интернета или оставить самостоятельной и изолированной от внешнего доступа.

Для доступа к ресурсам в домене применяется полное имя узла, например **zeta.webatwork.com**. Здесь **zeta** — имя индивидуального компьютера, **webatwork** — домен организации, а **com** — домен верхнего уровня. Домены верхнего уровня составляют фундамент иерархии DNS и потому называются ***корневыми доменами*** (root domains). Они организованы географически, с названиями на основе двухбуквенных кодов стран (ru для России), по типу организации *(com* для коммерческих организаций) и по назначению *(*mil для военных организаций).

Обычные домены, например, microsoft.com, называются ***родительскими*** (parent domain), поскольку они образуют основу организационной структуры. Родительские домены можно разделить на поддомены разных отделений или удаленных филиалов. Например, полное имя компьютера в офисе Microsoft в Сиэтле может быть **jacob.seattle.microsoft.com***,* где **jacob** — имя компьютера, **sealtle** — поддомен, а **microsoft.com** — родительский домен. Другое название поддомена — ***дочерний домен*** (child domain).

Компоненты Active Directory

Active Directory объединяет физическую и логическую структуру для компонентов сети. Логические структуры Active Directory помогают организовывать объекты каталога и управлять сетевыми учетными записями и общими ресурсами. К логической структуре относятся следующие элементы:

- ***организационное подразделение (organizational unit)*** — подгруппа компьютеров, как правило, отражающая структуру компании;
- ***домен (domain)*** — группа компьютеров, совместно использующих общую БД каталога;
- ***дерево доменов (domain tree)*** — один или несколько доменов, совместно использующих непрерывное пространство имен;

- ***лес доменов (domain forest)*** — одно или несколько деревьев, совместно использующих информацию каталога.

Физические элементы помогают планировать реальную структуру сети. На основании физических структур формируются сетевые связи и физические границы сетевых ресурсов. К физической структуре относятся следующие элементы:

• ***подсеть (subnet)*** — сетевая группа с заданной областью IP- адресов и сетевой маской;

• ***сайт (site)*** — одна или несколько подсетей. Сайт используется для настройки доступа к каталогу и для репликации.

Организационные подразделения

Организационные подразделения (ОП) — это подгруппы в доменах, которые часто отражают функциональную структуру организации. ОП представляют собой своего рода логические контейнеры, в которых размещаются учетные записи, общие ресурсы и другие ОП. Например, можно создать в домене **microsoft.com** подразделения **Resourses, IT**, **Marketing**. Потом эту схему можно расширить, чтобы она содержала дочерние подразделения.

В ОП разрешается помещать объекты только из родительского домена. Например, ОП из домена **Seattle.microsoft.com** содержат объекты только этого домена. Добавлять туда объекты из **my.microsoft.com** нельзя. ОП очень удобны при формировании функциональной или бизнес – структуры организации. Но это не единственная причина их применения.

ОП позволяют определять групповую политику для небольшого набора ресурсов в домене, не применяя ее ко всему домену. С помощью ОП создаются компактные и более управляемые представления объектов каталога в домене, что помогает эффективнее управлять ресурсами.

ОП позволяют делегировать полномочия и контролировать административный доступ к ресурсам домена, что помогает задавать пределы полномочий администраторов в домене. Можно передать пользователю **A** административные полномочия только для одного ОП и в то же время передать пользователю **B** административные полномочия для всех ОП в домене.

Домены

Домен Active Directory — это группа компьютеров, совместно использующих общую БД каталога. Имена доменов Active Directory должны быть уникальными. Например, не может быть двух доменов **microsoft.com**, но может быть родительский домен **microsoft.com** с дочерними доменами **seattle.microsoft.com** и **my.microsoft.com**. Если домен является частью закрытой сети, имя, присвоенное новому домену, не должно конфликтовать ни с одним из существующих имен доменов в этой сети. Если домен — часть глобальной сети Интернет, то его имя не должно конфликтовать ни с одним из существующих имен доменов в Интернете. Чтобы гарантировать уникальность имен в Интернете, имя родительского домена необходимо зарегистрировать через любую полномочную регистрационную организацию.

В каждом домене действуют собственные политики безопасности и доверительные отношения с другими доменами. Зачастую домены распределяются по нескольким физическим расположениям, т. е. состоят из нескольких сайтов, а сайты —

объединяют несколько подсетей. В БД каталога домена хранятся объекты, определяющие учетные записи для пользователей, групп и компьютеров, а также общие ресурсы, например принтеры и папки.

Функции домена ограничиваются и регулируются режимом его функционирования.

Леса и деревья

Каждый домен Active Directory обладает DNS-именем типа **microsoft.com.** Домены, совместно использующие данные каталога, образуют **лес** (forest). Имена доменов леса в иерархии имен DNS бывают *несмежными* (discontiguous) или *смежными* (contiguous).

Домены, обладающие смежной структурой имен, называют деревом доменов. Если у доменов леса несмежные DNS-имена, они образуют отдельные деревья доменов в лесу. В лес можно включить одно или несколько деревьев. Для доступа к доменным структурам предназначена консоль Active Directory — домены и доверие (Active Directory Domains and Trusts).

Функции лесов ограничиваются и регулируются функциональным режимом леса.

Сайты и подсети

Сайт — это группа компьютеров в одной или нескольких IP-подсетях, используемая для планирования физической структуры сети. Планирование сайта происходит независимо от логической структуры домена. Active Directory позволяет создать множество сайтов в одном домене или один сайт, охватывающий множество доменов.

В отличие от сайтов, способных охватывать множество областей IP-адресов, подсети обладают заданной областью IP-адресов и сетевой маской. Имена подсетей указываются в формате ***сеть/битовая маска,*** например 192.168.19.0/24, где сетевой адрес 192.168.19.0 и сетевая маска 255.255.255.0 скомбинированы в имя подсети 192.168.19.0/24.

Компьютеры приписываются к сайтам в зависимости от местоположения в подсети или в наборе подсетей. Если компьютеры в подсетях способны взаимодействовать на достаточно высоких скоростях, их называют ***хорошо связанными*** (well connected).

В идеале сайты состоят из хорошо связанных подсетей и компьютеров, если скорость обмена между подсетями и компьютерами низка, может потребоваться создать несколько сайтов. Хорошая связь дает сайтам некоторые преимущества.

- Когда клиент входит в домен, в процессе аутентификации сначала производится поиск локального контроллера домена в сайте клиента, т. е. по возможности первыми опрашиваются локальные контроллеры, что ограничивает сетевой трафик и ускоряет аутентификацию.
- Информация каталога реплицируется чаще ***внутри*** сайтов, чем ***между*** сайтами. Это снижает межсетевой трафик, вызванный репликацией, и гарантирует, что локальные контроллеры доменов быстро получат обновленную информацию.

Можно настроить порядок репликации данных каталога, используя ***связи сайтов*** (site links). Например, определить ***сервер-плацдарм*** (bridgehead) для репликации между сайтами.

Основная часть нагрузки от репликации между сайтами ляжет на этот специализированный сервер, а не на любой доступный сервер сайта. Сайты и подсети настраиваются в консоли Active Directory — сайты и службы (Active Directory Sites and Services).

Практическая работа 4. Настройка безопасности агента SQL. Дополнительные параметры развертывания и администрирования AD DS

Работа с доменами Active Directory

В сети Windows Server служба Active Directory настраивается одновременно с DNS. Тем не менее у доменов Active Directory и доменов DNS разное назначение. Домены Active Directory помогают управлять учетными записями, ресурсами и защитой.

Иерархия доменов DNS предназначена, главным образом, для разрешения имен.

Система Windows Server функционирует как контроллер домена или как рядовой сервер. Рядовые серверы становятся контроллерами после установки Active Directory; контроллеры понижаются до рядовых серверов после удаления Active Directory.

Оба процесса выполняет мастер установки Active Directory. В домене может быть несколько контроллеров. Они реплицируют между собой данные каталога по модели репликации с несколькими хозяевами, которая позволяет каждому контроллеру обрабатывать изменения каталога, а затем передавать их на другие контроллеры. Благодаря структуре с несколькими хозяевами все контроллеры по умолчанию обладают равной ответственностью. Впрочем, можно предоставить некоторым контроллерам домена приоритет над другими в определенных задачах, например, создать сервер-плацдарм, который обладает приоритетом при репликации данных каталога на другие сайты.

Кроме того, некоторые задачи лучше выполнять на выделенном сервере. Сервер, обрабатывающий специфический тип задач, называется ***хозяином операций*** (operations master).

Для всех компьютеров с Windows, присоединенных к домену, создаются учетные записи, хранящиеся, подобно другим ресурсам, в виде объектов Active Directory. Учетные записи компьютеров служат для управления доступом к сети и ее ресурсам, Прежде чем компьютер получает доступ к домену по своей учетной записи, он в обязательном порядке проходит процедуру аутентификации.

Структура каталога

Данные каталога предоставляются пользователям и компьютерам через ***хранилище данных*** (data stores) и ***глобальные каталоги*** (global catalogs). Хотя большинство функций Active Directory затрагивают хранилище данных, глобальные каталоги (ГК) не менее важны, поскольку используются для входа в систему и поиска информации. Если ГК недоступен, обычные пользователи не смогут войти в домен.

Единственный способ обойти это условие — локальное кэширование членства в универсальных группах.

Доступ и распространение данных Active Directory обеспечиваются средствами ***протоколов доступа к каталогу*** (directory access protocols) и ***репликации*** (replication).

Репликация нужна для распространения обновленных данных на контроллеры. Главный метод распространения обновлений — репликация с несколькими хозяевами, но некоторые изменения обрабатываются только специализированными контроллерами — ***хозяевами операций*** (operations masters).

Способ выполнения репликации с несколькими хозяевами в Windows Server также изменился благодаря появлению ***разделов каталога приложений*** (application directory partitions). Посредством их системные администраторы могут создавать в лесу доменов разделы репликации, которые представляют собой логические структуры, используемые для управления репликацией в пределах леса доменов. Например, можно создать раздел, который будет ведать репликацией информации DNS в пределах домена. Другим системам домена репликация информации DNS запрещена.

Разделы каталога приложений могут быть дочерним элементом домена, дочерним элементом другого прикладного раздела или новым деревом в лесу доменов. Реплики разделов разрешается размещать на любом контроллере домена Active Directory, включая глобальные каталоги. Хотя разделы каталога приложений полезны в больших доменах и лесах, они увеличивают издержки на планирование, администрирование и сопровождение.

Хранилище данных

Хранилище содержит сведения о важнейших объектах службы каталогов Active Directory — учетных записях, общих ресурсах, ОП и групповых политиках. Иногда хранилище данных называют просто ***каталогом*** (directory). На контроллере домена каталог хранится в файле NTDS.DIT, расположение которого определяется при установке Active Directory (это обязательно должен быть диск NTFS). Некоторые данные каталога можно хранить и отдельно от основного хранилища, например, групповые политики, сценарии и другую информацию, записанную в общем системном ресурсе SYSVOL.

Предоставление информации каталога в совместное пользование называют ***публикацией*** (publish). Например, открывая принтер для использования в сети, его публикуют; публикуется информация об общей папке и т. д. Контроллеры доменов реплицируют большинство изменений в хранилище по схеме с несколькими хозяевами. Администратор небольшой или среднего размера организации редко управляет репликацией хранилища, поскольку она осуществляется автоматически, но её можно настроить согласно специфике сетевой архитектуры.

Реплицируются не все данные каталога, а только:

- данные домена — информация об объектах в домене, включая объекты учетных записей, общих ресурсов, ОП и групповых политик;
- данные конфигурации — сведения о топологии каталога: список всех доменов, деревьев и лесов, а также расположение контроллеров и серверов ГК;

- данные схемы — информация обо всех объектах и типах данных, которые могут храниться в каталоге; стандартная схема Windows Server описывает объекты учетных записей, объекты общих ресурсов и др., её можно расширить, определив новые объекты и атрибуты или добавив атрибуты для существующих объектов.

Глобальный каталог

Если локальное кэширование членства в универсальных группах не производится, вход в сеть осуществляется на основе информации о членстве в универсальной группе, предоставленной ГК.

Он также обеспечивает поиск в каталоге по всем доменам леса. Контроллер, выполняющий роль сервера ГК, хранит полную реплику всех объектов каталога своего домена и частичную реплику объектов остальных доменов леса.

Для входа в систему и поиска нужны лишь некоторые свойства объектов, поэтому возможно использование частичных реплик. Для формирования частичной реплики при репликации нужно передать меньше данных, что снижает сетевой трафик.

По умолчанию сервером ГК становится первый контроллер домена. Поэтому, если в домене только один контроллер, то сервер ГК и контроллер домена — один и тот же сервер. Можно расположить ГК на другом контроллере, чтобы сократить время ожидания ответа при входе в систему и ускорить поиск. Рекомендуется создать по одному ГК в каждом сайте домена.

Есть несколько способов решения этой проблемы. Разумеется, можно создать сервер ГК на одном из контроллеров домена в удаленном офисе. Недостаток этого способа — увеличение нагрузки на сервер ГК, что может потребовать дополнительных ресурсов и тщательного планирования времени работы этого сервера.

Другой способ решения проблемы — локальное кэширование членства в универсальных группах. При этом любой контроллер домена может обслуживать запросы на вход в систему локально, не обращаясь к серверу ГК. Это ускоряет процедуру входа в систему и облегчает ситуацию в случае выхода сервера ГК из строя. Кроме того, при этом снижается трафик репликации.

Вместо того чтобы периодически обновлять весь ГК по всей сети, достаточно обновлять информацию в КЭШе о членстве в универсальной группе. По умолчанию обновление происходит каждые восемь часов на каждом контроллере домена, в котором используется локальное кэширование членства в универсальной группе.

Членство в универсальной группе индивидуально для каждого сайта. Напомним, что сайт — это физическая структура, состоящая из одной или нескольких подсетей, имеющих индивидуальный набор IP-адресов и сетевую маску. Контроллеры домена Windows Server и ГК, к которому они обращаются, должны находиться в одном сайте. Если есть несколько сайтов, придется настроить локальное кэширование на каждом из них. Кроме того, пользователи, входящие в сайт, должны быть частью домена Windows Server, работающего в режиме леса Windows Server.

Репликация в Active Directory

В каталоге хранятся сведения трех типов: данные домена, данные схемы и данные конфигурации. Данные домена реплицируются на все контроллеры домена. Все контроллеры домена равноправны, т.е. все вносимые изменения с любого контроллера домена будут реплицированы на все остальные контроллеры домена. Схема и

данные конфигурации реплицируются на все домены дерева или леса. Кроме того, все объекты индивидуального домена и часть свойств объектов леса реплицируются в ГК. Это означает, что контроллер домена хранит и реплицирует схему для дерева или леса, информацию о конфигурации для всех доменов дерева или леса и все объекты каталога и свойства для собственного домена.

Контроллер домена, на котором хранится ГК, содержит и реплицирует информацию схемы для леса, информацию о конфигурации для всех доменов леса и ограниченный набор свойств для всех объектов каталога в лесу (он реплицируется только между серверами ГК), а также все объекты каталога и свойства для своего домена.

Чтобы понять суть репликации, рассмотрим такой сценарий настройки новой сети.

1. В домене А установлен первый контроллер. Этот сервер — единственный контроллер домена. Он же является и сервером ГК. Репликация в такой сети не происходит, поскольку нет других контроллеров.
2. В домене А устанавливается второй контроллер, и начинается репликация. Можно назначить один контроллер хозяином инфраструктуры, а другой — сервером ГК. Хозяин инфраструктуры следит за обновлениями ГК и запрашивает их для измененных объектов. Оба этих контроллера также реплицируют данные схемы и конфигурации.
3. В домене А устанавливается третий контроллер, на котором нет ГК. Хозяин инфраструктуры следит за обновлениями ГК, запрашивает их для измененных объектов, а затем реплицирует изменения на третий контроллер домена. Все три контроллера также реплицируют данные схемы и конфигурации.
4. Создается новый домен Б, в него добавляются контроллеры. Серверы ГК в домене А и домене Б реплицируют все данные схемы и конфигурации, а также подмножество данных домена из каждого домена. Репликация в домене А продолжается, как описано выше, плюс начинается репликация внутри домена Б.

Active Directory и LDAP

Упрощенный протокол доступа к каталогам (Lightweight Directory Access Protocol, LDAP) — стандартный протокол Интернет соединений в сетях TCP/IP. LDAP спроектирован специально для доступа к службам каталогов с минимальными издержками. В LDAP также определены операции, используемые для запроса и изменения информации каталога.

Клиенты Active Directory применяют LDAP для связи с компьютерами, на которых работает Active Directory, при каждом входе в сеть или поиске общих ресурсов. LDAP упрощает взаимосвязь каталогов и переход на Active Directory с других служб каталогов. Для повышения совместимости можно использовать интерфейсы служб Active Directory (Active Directory Service- Interfaces, ADSI).

Роли хозяина операций

Хозяин операций решает задачи, которые неудобно выполнять в модели репликации с несколькими хозяевами. Существует пять ролей хозяина операций, которые можно назначить одному или нескольким контроллерам доменов. Одни роли должны

быть уникальны на уровне леса, для других достаточно уровня домена. В каждом лесе Active Directory должны существовать следующие роли:

- ***Хозяин схемы (schema master)*** — управляет обновлениями и изменениями схемы каталога. Для обновления схемы каталога необходим доступ к хозяину схемы. Чтобы определить, какой сервер в данное время является хозяином схемы в домене, достаточно открыть окно командной строки и ввести: dsquery server – hasfsmo schema.
- ***Хозяин именования доменов (domain naming master)*** — управляет добавлением и удалением доменов в лесу. Чтобы добавить или удалить домен, требуется доступ к хозяину именования доменов. Чтобы определить, какой сервер в данное время является хозяином именования доменов, достаточно в окне командной строки ввести: dsquery server –hasfsmo name.

Эти роли, общие для всего леса в целом, должны быть в нем уникальными.

В каждом домене Active Directory в обязательном порядке существуют следующие роли.

- Хозяин относительных идентификаторов (relative ID master) — выделяет относительные идентификаторы контроллерам доменов. Каждый раз при создании объекта пользователя, группы или компьютера контроллеры назначают объекту уникальный идентификатор безопасности, состоящий из идентификатора безопасности домена и уникального идентификатора, который был выделен хозяином относительных идентификаторов. Чтобы определить, какой сервер в данное время является хозяином относительных идентификаторов в домене, достаточно в окне командной строки ввести: dsquery server –hasfsmo rid**.**
- ***Эмулятор PDC (PDC emulator)*** — в смешанном или промежуточном режиме домена действует как главный контроллер домена Windows NT. Он аутентифицирует вход в Windows NT, обрабатывает изменения пароля и реплицирует обновления на PDC. Чтобы определить, какой сервер в данное время является эмулятором PDC в домене, достаточно в окне командной строки ввести dsquery server –hasfsmo pdc**.**
- ***Хозяин инфраструктуры (infrastructure master)*** — обновляет ссылки объектов, сравнивая данные своего каталога с данными ГК. Если данные устарели, он запрашивает из ГК обновления и реплицирует их на остальные контроллеры в домене. Чтобы определить, какой сервер в данное время является хозяином инфраструктуры в домене, достаточно в окне командной строки и ввести dsqueryserver –hasfsmo infr.

Эти роли, общие для всего домена, должны быть в нем уникальными. Иными словами, можно настроить только один хозяин относительных идентификаторов, один эмулятор PDC и один хозяин инфраструктуры для каждого домена.

Обычно роли хозяина операций назначаются автоматически, но их можно переназначить. При установке новой сети все роли хозяев операций получает первый контроллер первого домена. Если позднее будет создан новый дочерний домен или корневой домен в новом дереве, роли хозяина операций также автоматически назначаются первому контроллеру домена. В новом лесу доменов контроллеру домена назначаются все роли хозяина операций. Если новый домен создается в том же лесу, его контроллеру назначаются роли хозяина относительных идентификаторов, эмулятора PDC и хозяина инфраструктуры. Роли хозяина схемы и хозяина именования доменов остаются у первого домена леса.

Если в домене только один контроллер, он выполняет все роли хозяев операций. Если в сети один сайт, стандартное расположение хозяев операций оптимально. Но по мере добавления контроллеров домена и доменов иногда требуется переместить роли хозяев операций на другие контроллеры доменов.

Если в домене два или более контроллеров, рекомендуется сконфигурировать два контроллера домена для выполнения ролей хозяина операций. Например, назначить один контроллер домена основным хозяином операций, а другой — запасным, который понадобится при отказе основного.

Администрирование Active Directory

С помощью службы Active Directory создаются учетные записи компьютеров, проводится подключение их к домену, производится управление компьютерами, контроллерами домена и организационными подразделениями (ОП).

Для управления Active Directory предназначены средства администрирования и поддержки. Перечисленные ниже инструменты реализованы и виде оснасток консоли MMC (Microsoft Management Console):

- ***Active Directory — пользователи и компьютеры (Active Directory Users and Computers)*** позволяет управлять пользователями, группами, компьютерами и организационными подразделениями (ОП);
- ***Active Directory — домены и доверие (Active Directory Domains and Trusts)*** служит для работы с доменами, деревьями доменов и лесами доменов;
- ***Active Directory — сайты и службы (Active Directory Sites and Services)*** позволяет управлять сайтами и подсетями;
- ***Результирующая политика (Resultant Set of Policy)*** используется для просмотра текущей политики пользователя или системы и для планирования изменений в политике.

Утилиты командной строки Active Directory

Для управления объектами Active Directory существуют средства командной строки, которые позволяют осуществлять широкий спектр административных задач:

- ***DSADD*** — добавляет в Active Directory компьютеры, контакты, группы, ОП и пользователей.
- ***DSGET*** — отображает свойства компьютеров, контактов, групп, ОП, пользователей, сайтов, подсетей и серверов, зарегистрированных в Active Directory.
- ***DSMOD*** — изменяет свойства компьютеров, контактов, групп, ОП, пользователей и серверов, зарегистрированных в Active Directory.
- ***DSMOVE*** — перемещает одиночный объект в новое расположение в пределах домена или переименовывает объект без перемещения.
- ***DSQXJERY*** — осуществляет поиск компьютеров, контактов, групп, ОП, пользователей, сайтов, подсетей и серверов в Active Directory по заданным критериям.
- ***DSRM*** — удаляет объект из Active Directory.
- ***NTDSUTIL*** — позволяет просматривать информацию о сайте, домене или сервере, управлять ***хозяевами операций*** (operations masters) и обслуживать базу данных Active Directory.

Вопросы по теме: Основные понятия Active Directory

1. Какой компьютер называется контроллером домена?
2. Какая система имен используется в Active Directory?
3. Что составляет фундамент иерархии DNS?
4. Перечислите принципы организации доменов верхнего уровня?
5. Что относится к логической структуре AD?
6. Что формируется на основании физических структур AD?
7. Какие элементы относятся к физической структуре AD?
8. Что представляют собой организационные подразделения?
9. Какие объекты разрешается помещать в организационные подразделения?
10. Что подразумевается под понятием домен Active Directory?
11. Какая особенность должна быть у имен доменов Active Directory?
12. Что хранится в БД каталога домена?
13. Какие бывают имена доменов леса в иерархии имен DNS?
14. Что называют деревом доменов?
15. Дайте определение сайта.
16. Как происходит планирование сайта?
17. Чем обладают подсети?
18. Какие компьютеры называют хорошо связанными?
19. Для чего используются связи сайтов?
20. Как настраивается служба Active Directory?
21. В чем проявляется разное назначение у доменов Active Directory и доменов DNS?
22. Что происходит с компьютерами при помощи Active Directory?
23. Что называется хозяином операции?

24. Для чего служат учетные записи компьютеров?

25. Через какие объекты данные каталога предоставляются пользователям и компьютерам?

26. Для чего используются глобальные каталоги?

27. Чем обеспечиваются доступ и распространение данных Active Directory?

28. Для чего нужна репликация?

29. Что содержит хранилище данных?

30. Что называют публикацией?

31. Какие данные каталога реплицируются?

32. Какие роли должны существовать в каждом лесе Active Directory?

Практическая работа 5. Сертификаты безопасности: виды, функции, срок действия. Проверка наличия сертификата безопасности

СИСТЕМЫ СЕРТИФИКАЦИИ

Сертификация программного обеспечения - это подтверждение соответствия показателей надежности, мобильности, эффективности, корректности и других его характеристик, а также заявленных свойств требованиям нормативных документов (например,в соответствии с ГОСТ 28195-89 или ГОСТ Р ИСО/МЭК 9126-93).

Основной целью сертификации программных средств и систем качества,обеспечивающих их жизненный цикл, является контроль и удостоверение качества технологий и продукции, гарантирование их высоких потребительских свойств.

Целью сертификации является подготовка и принятие решения о целесообразности выдачи заявителю сертификата соответствия с учетом следующих факторов:

- полноты, точности и достоверности исходного технического задания и спецификаций требований, представленных в документации на ПС, а также на технологию поддержки его жизненного цикла;
- достоверности и точности измерения и обобщения результатов сертификационных испытаний и получения адекватных показателей качества конечных программных продуктов и/или технологических процессов их создания;
- методологии и качества интерпретации данных об объекте испытаний и/или технологии с учетом достоверности оценок, квалификации и объективности испытателей, заказчиков и пользователей.

Общие правовые основы сертификации продукции и услуг в Российской Федерации установлены Законом "О сертификации продукции и услуг", Федеральным Законом от 27.12.2002 № 184-ФЗ «О техническом регулировании» где определены права и ответственность в области сертификации органов государственного управления, а такжеизготовителей (продавцов, исполнителей) и других участников сертификации.

Результатом положительных испытаний является ***сертификат соответствия*** - документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям. Сертификация программных средств и систем является элементом общей системы сертификации продукции в РоссийскойФедерации.

Система сертификации — система, располагающая собственными правилами процедуры и управления для проведения сертификации.

Орган по сертификации — орган, проводящий сертификацию соответствия. Орган посертификации может сам проводить испытания или же осуществлять надзор за этой деятельностью, проводимой по его поручению другими органами.

Организационная структура системы сертификации в России включает:

1. государственный (национальный) орган по сертификации,
2. ведомственные органы по управлению сертификацией продукции определенныхклассов,
3. испытательные центры (лаборатории).

Национальным органом по сертификации продукции в Российской Федерации является **Госстандарт России**, который осуществляет следующие *функции*:

- организует ведение обязательной сертификации продукции по поручению органов законодательной или исполнительной власти;
- организует и финансирует разработку, а также утверждает основополагающие нормативно-технические и методические документы системы сертификации;
- утверждает документы, устанавливающие порядок сертификации конкретных видов продукции;
- проводит аккредитацию испытательных центров (лабораторий) совместно с ведомственными органами по сертификации и выдает аттестат аккредитации;
- признает иностранные сертификаты соответствия, осуществляет взаимодействие с соответствующими уполномоченными органами других стран и международных организацийпо вопросам сертификации;
- регистрирует и аннулирует сертификаты соответствия и сертификационные лицензии,рассматривает спорные вопросы, возникающие в процессе сертификации;

- организует периодическую публикацию информации по сертификации.

Основой сертификации продукции в Российской Федерации является Системасертификации ГОСТ Р Госстандарта России.

Виды сертификации

Сертификация проводится для подтверждения соответствия программного продукта государственным стандартам в области информационных технологий (набор стандартов, на соответствие которым будет проверяться ПС, согласуется с заказчиком), требованиям технических условий, технического задания.

Выделяют два вида сертификации:

1) *Обязательная сертификация* — подтверждение уполномоченным на то органом соответствия продукции обязательным требованиям, установленным законодательством. Обязательная сертификация является формой государственного контроля за безопасностью продукции. Поэтому она может осуществляться лишь в случаях, предусмотренных законодательными актами РФ.

2) *Добровольная сертификация* проводится в соответствии с Законом РФ по инициативе заявителей (изготовителей, продавцов, исполнителей) в целях подтверждения соответствия продукции (услуг) требованиям стандартов, технических условий, рецептур и других документов, определяемых заявителем.

В зависимости от области применения системы, от назначения и класса ПС, их сертификация может быть ***обязательной*** или ***добровольной***.

В соответствии с действующими законодательными и нормативными документами сертификация средств информатизации проводится в Российской Федерации в следующих основных направлениях:

- *обязательная сертификация средств информатизации* на соответствие требованиям электромагнитной совместимости, а также требованиям, обеспечивающим безопасность жизни, здоровья, имущества потребителей и охрану среды обитания;
- *обязательная сертификация средств защиты информации*;
- *добровольная сертификация* функциональных параметров средств и систем информатизации, по номенклатуре и характеристикам, устанавливаемым отраслевыми (фирменными) стандартами, и учитывающим различные аспекты применения аппаратуры и программного обеспечения.

Добровольная сертификация применяется для средств информатизации, не подлежащих в соответствии с законодательными актами Российской Федерации обязательнойсертификации, и проводится по требованиям, на соответствие которым законодательными актами Российской Федерации не предусмотрено проведение обязательной сертификации. Добровольная сертификация проводится для удостоверения

качества средств и систем информатизации с целью повышения их конкурентоспособности, расширения сферыиспользования и получения дополнительных экономических преимуществ.

В сфере информатизации создан эффективный инструмент оценки уровня качества приобретаемых средств информатизации в виде Системы добровольной сертификации средств и систем информатизации "Росинфосерт". Система сертификации "Росинфосерт"создана в 1994 году Комитетом при Президенте Российской Федерации по политике информатизации (РОСКОМИНФОРМОМ) и внесена в Государственный реестр систем сертификации, действующих в Российской Федерации.

В соответствии с действующим законодательством РоссийскойФедерации сертификации программного обеспечения проводится ***только в добровольной системе сертификации*** продукции. Продукция, на которую получен сертификат на программное обеспечение пользуется большим доверием, так как данный документ подтверждает высокое качество продукта, его надежность и соответствие требованиям государственных стандартов.

Сертификация программ может быть проведена для таких видов продукции:

- сетевое программное обеспечение;
- системы управления базой данных;
- операционные системы и средства расширения;
- программное обеспечение для моделирования;
- программное обеспечение для электронных сделок;
- программное обеспечение для обработки документов;
- программное обеспечение для автоматизации управления объединения и отраслями;
- информационно-справочные системы и базы данных;
- программное обеспечение для презентационной графики;
- утилиты и системы программирования;
- системы автоматизированного проектирования;
- аукционы, лотереи, игры, развлечения и др.;
- электронные издания;
- приложения мультимедиа;
- педагогическое программное обеспечение;
- программное обеспечение для технологической подготовки производства и многиедругие.

Процедура сертификации

Для удостоверения качества конечного продукта – программных средств и их компонентов, следует сертифицировать технологические процессы, обеспечивающих их жизненный цикл. Поэтому необходимо рассматривать совместно задачисертификации ***конечных объектов – программных продуктов***, а также ***технологий и системкачества***, обеспечивающих их создание и совершенствование.

В исходных нормативных документах и требованиях должны быть сосредоточены ***все функциональные и эксплуатационные характеристики***, обеспечивающие заказчику и пользователям возможность корректного применения сертифицированного объекта и/илитехнологического процесса во всем многообразии его функций и характеристик качества.

Сертификационные испытания являются наиболее формализованным и регламентированным этапом тестирования, как ***объектов*** □ программных продуктов, таки ***процессов*** их создания, поддерживаемым значительным числом стандартов и документов. При сертификации обычно ***руководствуются следующими основными исходными документами:***

- действующими международными, государственными и ведомственными стандартами на проектирование и испытания комплексов программ, на жизненный цикл ПС, системы обеспечения и характеристики их качества, а также на технологическую документацию;
- утвержденным заказчиком и согласованным с разработчиком техническим заданием и/или спецификацией требований, утвержденным комплектом эксплуатационной документации на ПС и его компоненты, а также на систему обеспечения их качества;
- Программой сертификационных испытаний по всем требованиям техническогозадания и положениям эксплуатационной документации;
- методиками испытаний по каждому разделу требований технического задания идокументации.

Сертификация состоит из ряда организационных процессов, составляющих ***Систему сертификации***, которые поддерживаются регламентированными процедурами и документами и должны выполняться квалифицированными, аттестованными экспертами – инспекторами.

Процесс сертификации программных продуктов и систем качества предприятия включает:

1. анализ и выбор разработчиком или заказчиком (заявителем), компетентных в данной области органа и аттестованной лаборатории для выполнения сертификационных испытаний;
2. подачу заявителем заявки на испытания в орган сертификации и при-

нятиесертификаторами решения по заявке, выбор схемы сертификации, заключение договора на сертификацию;

3. идентификацию требований к системе качества предприятия и/или к версии программного продукта, подлежащих испытаниям;
4. выполнение сертификационных испытаний системы качества предприятия или версии программного продукта сертификационной лабораторией;
5. анализ полученных результатов и принятие решения лабораторией и/или органом сертификации о возможности выдачи заявителю сертификата соответствия;
6. выдачу органом сертификации заявителю – сертификата и лицензии на применение знака соответствия и на выпуск сертифицированной продукции – версий программного продукта;
7. осуществление инспекционного контроля органом сертификации сертифицированной системы качества предприятия и/или продукции;
8. проведение заявителем корректирующих мероприятий при нарушении соответствия процессов системы качества и/или продукции установленным требованиям и при неправильном применении знака соответствия.

На сертификацию принимаются только рабочие версии программных продуктов (т.е., версии, не содержащие ограничений по времени работы и других параметров).

Вместе с заявкой необходимо предоставить в орган по сертификации следующие обязательные документы и материалы:

- письменное подтверждение согласия с процедурой сертификации, подписанное руководителем организации-заявителя (заявителем);
- письменное согласие от организации, разработавшей программный продукт (в случае,если заявка подана от имени организации эксплуатирующей или продающей программный продукт);
- «Техническое задание» по ГОСТ 19.201-78;
- «Спецификация» по ГОСТ 19.202-78;
- «Описание программы» по ГОСТ 19.402-78;
- «Описание применения» по ГОСТ 19.502-78;
- «Руководство пользователя» по РД 50-34.698-90;
- «Программа и методика испытаний» по ГОСТ 19.301-79;
- акт проведения испытаний;
- две дистрибутивные копии программного средства. Дистрибутивы должны

сопровождаться отпечатанным списком файлов, записанных надискетах и компакт дисках, в списке должны быть указаны объем файлов, дата и времяих создания;

- копия документа (лицензии), подтверждающего легальность покупки фирмой- разработчиком инструментальных и общесистемных программных средств (ОС, СУБД, языкипрограммирования), использованных для разработки программных продуктов,предоставленных на сертификацию.

Сертификационные испытания ПС осуществляется в два этапа:

1. Технологические испытания. Проводятся с использованием современныхметодов и средств по формализованным правилам, удостоверяющим соответствие реальных количественных и качественных показателей тем, которые зафиксированы в НТД или программной документации;

2. Оценка, проводимая экспертами.В ходе испытаний выполняется:

- Идентификация объекта испытаний путем проверки характеристик идентификации программного средства (полное название ПС, версия и дата выпуска ПС, сведения о разработчике ПС, сведения о входящих в состав компонентах, основные выполняемые функции, состав программной документации);
- Инсталляция путем установки программного продукта на компьютеры, на которые доэтого данный программный продукт не был установлен;
- Экспертиза программной документации на соответствие требованиям Государственных стандартов ГОСТ Р ИСО/МЭК 12119-2000 (п. 3.2), ГОСТ Р ИСО 9127-94 (п.п. 5, 6.1, 6.3-6.5);
- Проверка и оценка качества сертифицируемого программного продукта в соответствии с требованиями нормативных документов (список документов определяется в процессе разработки методики), проверка программного продукта на соответствие выполняемых функций по руководству пользователя и требованиям технического задания.

На основании испытаний оцениваются полученные результаты и обосновываются выводы о соответствии или несоответствии продукции или процессов требованиям нормативных документов. Протоколы испытаний представляются в орган по сертификации, атакже заявителю по его требованию. Протоколы испытаний подлежат хранению в течение сроков, установленных в правилах систем сертификации продукции и в документах испытательной лаборатории, но не менее трех лет.

Протоколы испытаний представляются заявителю и в орган по сертификации.Заявитель может представить в орган по сертификации протоколы испытаний с учетом срокових действия, проведенных при разработке и постановке продукции на производство, или документы об испытаниях, выполненных отечественными или зарубежными испытательнымилабораториями, аккредитованными или признанными в

Системе сертификации. На основании протоколов сертификационных испытаний оцениваются полученные результаты и обосновываются сделанные выводы о соответствии или несоответствии продукции требованиям нормативных документов.

Заключение по результатам сертификационных испытаний разрабатывается сертификаторами и содержит обобщенные сведения о результатах испытаний и обоснование целесообразности выдачи сертификата. В случае получения отрицательных результатов сертификационных испытаний принимается решение об отказе в выдаче сертификата соответствия. После доработки сертифицируемой продукции или системы качества испытания могут быть повторены. Результаты анализа состояния технологии или качества продукции ***оформляются актом***, в котором даются оценки по всем позициям Программы испытаний и содержатся выводы, включающие общую оценку состояния производства и продукции, необходимость корректирующих мероприятий. Акт используется органом посертификации наряду с протоколами испытаний, заявкой для выдачи и определения срока действия сертификата на программный продукт, периодичности инспекционного контроля, а также для составления корректирующих мероприятий.

По результатам сертификационных испытаний и экспертизы документации принимается ***решение о выдаче сертификата***. В случае получения отрицательных результатов сертификационных испытаний принимается ***решение об отказе в выдаче сертификата*** соответствия. Кроме того, предприятию-заявителю могут быть направлены предложения по устранению предполагаемых причин отрицательных результатов испытаний,после доработки сертифицируемой продукции испытания могут быть повторены.

Орган по сертификации после анализа протоколов испытаний, оценки производства, сертификации системы качества, анализа документации, указанной в решении по заявке, осуществляет оценку соответствия продукции установленным требованиям, ***оформляет сертификат*** на основании заключения экспертов и ***регистрирует его***. При внесении изменений в конструкторскую или эксплуатационную документацию, которые могутповлиять на качество системы или программный продукт, удостоверяемые при сертификации,заявитель должен известить об этом орган по сертификации, для принятия решения о необходимости проведения дополнительных испытаний. После регистрации сертификат вступает в силу и направляется предприятию-заявителю. Одновременно с выдачей сертификата предприятию-заявителю может выдаваться ***лицензия*** на право применения знака соответствия.

За сертифицированными программными продуктами в процессе их эксплуатациив течение всего срока действия сертификата соответствия должен осуществляться ***инспекционный контроль***. Инспекционный контроль проводится в форме периодических и внеплановых проверок соблюдения требований к качеству технологии и сертифицированной продукции. Объектами контроля, в зависимости от схемы сертификации,является сертифицированная продукция, система качества или стабильность производства предприятия-разработчика. При определении периодично-

сти и объема инспекционной проверки учитываются следующие факторы: степень потенциальной опасности программногопродукта, стабильность производства, объем выпуска, наличие и применение системы качества при разработке, информация о результатах испытаний продукта и его производства,проведенных изготовителем, органами государственного контроля и надзора.

Результаты инспекционного контроля ***оформляются актом***, в котором дается оценкарезультатов испытаний образцов и других проверок, делается общее заключение о состоянии производства сертифицированной продукции и возможности сохранения действиявыданного сертификата. Акт хранится в органе по сертификации, а его копии направляются разработчику и в организации, принимавшие участие в инспекционном контроле. По результатам инспекционного контроля ***орган по сертификации может приостановить илиотменить действие сертификата*** и аннулировать лицензию на право применения знака соответствия в случае несоответствия продукции требованиям нормативных документов,контролируемых при сертификации, а также в случаях:

- принципиальных изменений модели зрелости, профиля стандартов, нормативныхдокументов на продукцию или метода испытаний;
- изменения конструкции (состава), комплектности продукции;
- изменения организации или технологии разработки и производства;
- невыполнения требований технологии, методов контроля и испытаний, системы качества, если перечисленные изменения могут вызвать несоответствие продукции требованиям, контролируемым при сертификации.

Решение о приостановлении действия сертификата и лицензии на право применения знака соответствия не принимается в том случае, если путем корректирующих мероприятий, согласованных с органом по сертификации, его выдавшим, заявитель может устранить обнаруженные причины несоответствия и подтвердить без повторных испытаний в аккредитованной лаборатории, соответствие продукта или процессов нормативным документам. Если этого сделать нельзя, то действие сертификата отменяется, илицензия на право применения знака соответствия аннулируется. Информация о приостановлении или отмене действия сертификата доводится органом по сертификации, еговыдавшим, до сведения заявителя, потребителей и других заинтересованных организаций. Действие сертификата и право маркирования продукции знаком соответствия могут быть возобновлены при выполнении предприятием-разработчиком следующих условий:

- выявления причин несоответствия и их устранения;
- представления в орган по сертификации отчета о проделанной работе по улучшениюи обеспечения качества продукции;
- проведения по методикам и под контролем органа по сертификации дополнительныхиспытаний продукции и получения положительных результатов.

Задание.
Составьте по материалам лекции 15 - 20 вопросов с ответами и перешлите преподавателю

Практическая работа №6. Разработка политики безопасности корпоративной сети

Цель занятия: Познакомить обучающихся с основными приемами работы с политиками безопасности корпоративной сети;

Содержание и порядок выполнения задания:

Теоретический материал

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

Информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

- ***Конфиденциальность*** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- ***Целостность*** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- ***Доступность*** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. ***Атакой*** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - ***злоумышленником***. Потенциальные злоумышленники называются *источниками угрозы*.

Угрозы можно классифицировать по нескольким критериям:

- по *свойствам информации* (доступность, целостность, конфиденциальность),против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные,программы, аппаратура, *поддерживающая инфраструктура*);
- по способу осуществления (случайные/преднамеренные действияприродного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Угроза является следствием наличия **уязвимых мест илиуязвимостей** винформационной системе.

Причинами возникновения уязвимостей в общем случае являются:

1. ошибки при разработке программного обеспечения;
2. преднамеренные изменения программного обеспечения с целью внесенияуязвимостей;
3. неправильные настройки программного обеспечения;
4. несанкционированное внедрение вредоносных программ;
5. неумышленные действия пользователей;
6. сбои в работе программного и аппаратного обеспечения.

Уязвимости можно классифицировать по различным признакам:

1. по типу ПО – системное или прикладное.
2. По этапу жизненного цикла ПО, на котором возникла уязвимость –проектирование, эксплуатация и пр.
3. По причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов.
4. по характеру последствий от реализации атак – изменение прав доступа, подборпароля, вывод из строя системы в целом и пр.

Прежде чем приступать к построению системы защиты информации необходимо провести *анализ уязвимостей* ИС и попытаться сократить их количество, то есть использовать метод превентивности.

Важнейшие угрозы безопасности баз данных:

1. Чрезмерные и неиспользуемые пользовательские привилегии

Когда кто-либо получает привилегии, объемы которых превышают необходимые для выполнения должностных обязанностей, возникает вероятность злоупотребления этими привилегиями. Более того, когда какого-либо работника переводят на другую должность или онувольняется, уровень его доступа к конфиденциальной информации часто остается неизменным.

2. Злоупотребление привилегиями

Существует вероятность использования пользователями своих легитимных прав доступав противоправных целях.

3. Input-инъекции (инъекции в поле ввода)

Существует два основных способа взлома баз данных при помощи инъекций кода:

- SQL-инъекции, применяемые для взлома традиционных СУБД. SQL-

инъекцииобычно представляют собой внедрение (инъекцию) неразрешенного или вредоносного кода в поля ввода веб-приложений.

- NoSQL-инъекции, которые используются для взлома платформ Big Data. Инъекции типа NoSQL подразумевают внедрение вредоносного кода в компоненты Big Data (например, в Hive или MapReduce).

4. Хакерские программы

Киберпреступники, профессиональные хакеры применяют передовые методы атаки, сочетающие в себе различные тактические приемы, такие как фишинговые электронные письмаи хакерские программы, с целью проникновения в сеть организаций и получения конфиденциальных данных. Легитимные пользователи, не зная об инфицировании своих компьютеров хакерским ПО, могут стать невольными посредниками, при помощи которых хакеры получают доступ к сетям и важным данным.

5. Недостаточные меры по аудиту данных.

Корпоративная информационная система должна включать в себя средства для автоматической регистрации транзакций базы данных, в том числе протоколирования операций с конфиденциальной информацией. Отказ от сбора детальных данных аудита ведет к возникновению серьезных угроз на множестве уровней.

Многие организации используют встроенные в СУБД средства аудита, полагаются на узкоспециализированные решения или проводят аудит в ручном режиме. Однако возможности таких инструментов ограничены – они не позволяют проводить полноценный аудит, выявлять попытки взлома и проводить расследования. Более того, встроенные в СУБД средства часто оказывают излишнюю нагрузку на процессор и жесткий диск сервера, поэтому во многихслучаях функция аудита просто отключается. Наконец, большинство встроенных решений работают лишь на одной, предназначенной для них, платформе. Так, логи Oracle отличаются от логов MS-SQL, а логи MS-SQL отличаются от логов DB2. Это значительно осложняет внедрение однородного, масштабируемого механизма аудита в организациях, оперирующих СУБД различного типа.

Большинство встроенных инструментов аудита не способны определить конечного пользователя, поскольку ассоциируют активность БД с учетными записями клиентских приложений. Отсутствие связи с пользователем, совершившим ту или иную операцию, препятствует ведению отчетности, возможности наблюдения и проведению расследований. К тому же, пользователи, обладающие правами администратора БД (легитимными или полученными в результате взлома), могут отключить встроенный аудит, чтобы скрыть свою вредоносную активность. Именно поэтому необходимо разграничивать функции управления аудитом и администрирование БД и серверной платформы, чтобы добиться четкого разделения зон ответственности.

6. Незащищенность носителей информации.

Носители информации, предназначенные для хранения резервных копий, часто остаютсябез какой-либо защиты. Результатом этого становятся похищения дисков и пленок, содержащихрезервные копии баз данных.

7. Эксплуатация уязвимых, неверно сконфигурированных баз данных

На практике часто встречаются устаревшие версии баз данных и БД с настройками «по умолчанию». К сожалению, обновление баз данных часто игнорируется даже в тех случаях, когда выпускаются патчи и обновления.

8. Неуправляемая конфиденциальная информация

Неучтенные БД могут содержать важную информацию, могут появляться новые базы данных (например, в процессе тестирования системы) – и все это проходит незамеченным службой безопасности компании. Если вовремя не внедрить систему разграничения прав доступа, конфиденциальные данные, содержащиеся в этих базах данных, могут стать уязвимыми к взлому и утечкам.

9. Отказ в обслуживании (DoS).

DoS – это способ атаки информационной системы, в результате которой легитимные пользователи теряют доступ к сетевым приложениям или информации. Существуют различные способы создания DoS-условий. Наиболее популярным способом проведения DoS-атаки на базуданных является провокация перегрузки аппаратных ресурсов сервера, таких как память ипроцессор, путем его бомбардировки чрезмерно большим количеством запросов или меньшим по количеству запросов, но на обработку которых требуется непропорционально много системных ресурсов. В обоих случаях DoS-атака приводит к одному результату: сервер, столкнувшись с недостатком системных ресурсов, отказывает своим пользователям в обслуживании и в некоторых случаях даже «падает».

10. Недостаток знаний и опыта в сфере информационной безопасности.

Развитие средств внутренней безопасности не успевает за ростом объемов данных, при этом многие организации слишком плохо оснащены и подготовлены для противодействия угрозам. Причиной этого часто является недостаток опыта и квалификации сотрудников вприменении решений, улучшении политик или реагировании на инциденты в сфере безопасности.

В связи с повсеместным развитием Интернета наиболее часто атаки производятсяс использованием уязвимостей протоколов сетевого взаимодействия.

Наиболее распространенные атаки:

1. Анализ сетевого трафика

Данный вид атаки направлен в первую очередь на получение пароля и идентификатора пользователя путем "прослушивания сети". Реализуется это с помощью *sniffer* – специальная программа-анализатор, которая перехватывает все пакеты, идущие

по сети. И если протокол, например, FTP или TELNET, передает аутентификационную информацию в открытом виде, то злоумышленник легко получает доступ к учетной записи пользователя.

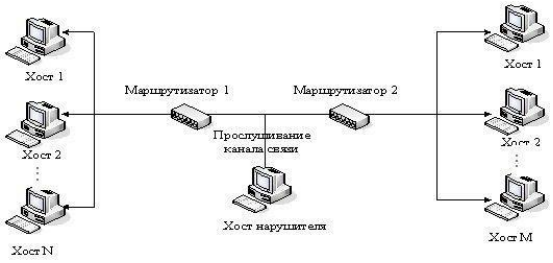


Рис. - Схема реализации угрозы "Анализ сетевого трафика"

2. Сканирование сети

Суть данной атаки состоит в сборе информации о топологии сети, об открытых портах, используемых протоколах и т.п. Как правило, реализация данной угрозы предшествует дальнейшим действиям злоумышленника с использованием полученных в результате сканирования данных.

Угроза выявления пароля

Целью атаки является преодоление парольной защиты и получении НСД к чужой информации. Методов для кражи пароля очень много: простой перебор всех возможных значений пароля, перебор с помощью специальных программ (*атака словаря*), перехват пароля с помощью программы-анализатора сетевого трафика.

3. **Подмена доверенного объекта сети и передача по каналам связи сообщенийот его имени с присвоением его прав доступа.** Доверенный объект – это элемент сети, легально подключенный к серверу.

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмыидентификации и аутентификации хостов, пользователей и т.д.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав *доверенного субъекта* взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени *доверенного субъекта*. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh- службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа, установленные его пользователем для доверенного абонента, к техническому средству ИС – цели угроз.

4. Навязывание ложного маршрута сети

Данная атака стала возможной из-за недостатков протоколов маршрутизации (RIP, OSPF, *LSP*) и управления сетью (ICMP, SNMP), таких как слабая аутентификация маршрутизаторов. Суть атаки состоит в том, что злоумышленник, используя уязвимости протоколов, вносит несанкционированные изменения в маршрутно-адресные таблицы.

5. Внедрение ложного объекта сети

Когда изначально объекты сети не знают информацию друг о друге, то для построения адресных таблиц и последующего взаимодействия, используется *механизм запрос* (как правило, широковещательный) - ответ с искомой информацией. При этом если нарушитель перехватил такой запрос, то он может выдать ложный ответ, изменить таблицу маршрутизации всей сети, и выдать себя за легального субъекта сети. В дальнейшем все пакеты, направленные к легальному субъекту, будут проходить через злоумышленника.

6. Отказ в обслуживании

Этот тип атак является одним из самых распространенных в настоящее время. Целью такой атаки является отказ в обслуживании, то есть нарушение доступности информации для законных субъектов информационного обмена.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИС на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по *протоколу ICMP* (Ping *flooding*), шторм запросов на установление TCP-соединений (SYN-*flooding*), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение *очередей запросов* на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения *очередей запросов*, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-*flooding*), шторм сообщений почтовому серверу (*Spam*);
- явный отказ в обслуживании, вызванный нарушением логической связности

между техническими средствами ИС при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-*flooding*) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "*Nuke*", "UDP-*bomb*") илиимеющих длину, превышающую максимально допустимый размер (угроза типа "Ping Death"), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Контрольные вопросы

1. Какие события безопасности должны фиксироваться в журнале аудита?
2. Какие параметры определяют политику аудита?
3. Целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
4. Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
5. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
6. Нужно ли ограничивать права пользователей по запуску прикладных программ и почему?
7. Какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?
8. Из каких этапов состоит построение политики безопасности для компьютерной системы?
9. К чему может привести ошибочное определение политики безопасности (приведите примеры)?
10. Почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной работе параметров политики безопасности?

Практическая работа №7. Получение сертификата

Цель занятия: Ознакомить обучающихся с основными понятиями работы в табличном редакторе, работе с БД в электронных таблицах

Содержание и порядок выполнения задания:

Теоретический материал

Что такое SSL-сертификат?

SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. Аббревиатура SSL означает Secure Sockets Layer – протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером.

Компаниям и организациям необходимо добавлять SSL-сертификаты на веб-сайты для защиты онлайн-транзакций и обеспечения конфиденциальности и безопасности клиентских данных.

SSL обеспечивает безопасность интернет-соединений и не позволяет злоумышленникам считывать или изменять информацию, передаваемую между двумя системами. Если в адресной строке рядом с веб-адресом отображается значок замка, значит этот веб-сайт защищен с помощью SSL.

С момента создания протокола SSL около 25 лет назад, он был доступен в нескольких версиях. При использовании каждой из этих версий в определенный момент возникали проблемы безопасности. Затем появилась обновленная переименованная версия протокола – TLS (Transport Layer Security), которая используется до сих пор. Однако аббревиатура SSL прижилась, поэтому новая версия протокола по-прежнему часто называется старым именем.

Как работают SSL-сертификаты?

Использование SSL гарантирует, что данные, передаваемые между пользователями и веб-сайтами или между двумя системами, невозможно прочитать сторонним лицам или системам. SSL использует алгоритмы для шифрования передаваемых данных, что не позволяет злоумышленникам считать их при передаче через зашифрованное соединение. Эти данные включают потенциально конфиденциальную информацию, такую как имена, адреса, номера кредитных карт и другие финансовые данные.

Процесс работает следующим образом:

1. Браузер или сервер пытается подключиться к веб-сайту (веб-серверу), защищенному с помощью SSL.
2. Браузер или сервер запрашивает идентификацию у веб-сервера.
3. В ответ веб-сервер отправляет браузеру или серверу копию своего SSL-сертификата.
4. Браузер или сервер проверяет, является ли этот SSL-сертификат доверенным. Если это так, он сообщает об этом веб-серверу.

5. Затем веб-сервер возвращает подтверждение с цифровой подписью и начинает сеанс, зашифрованный с использованием SSL.
6. Зашифрованные данные используются совместно браузером или сервером и веб-сервером.

Этот процесс иногда называют подтверждением SSL-соединения. Хотя по описанию этот процесс выглядит длительным, в реальности он занимает миллисекунды.

Если веб-сайт защищен SSL-сертификатом, в веб-адресе появляется аббревиатура HTTPS (безопасный протокол передачи гипертекста). Для сайтов без SSL-сертификата отображается аббревиатура HTTP, без буквы S, соответствующей Secure (безопасный). Также в адресной строке веб-адреса будет отображаться значок замка. Это свидетельствует о безопасности и обеспечивает уверенность посетителям веб-сайта.

Чтобы просмотреть сведения об SSL-сертификате, можно щелкнуть значок замка, расположенный на панели браузера. Данные, входящие в SSL-сертификат, обычно включают:

- Доменное имя, для которого выпущен сертификат.
- Лицо, организация или устройство, для которого выпущен сертификат.
- Центр сертификации, выдавший сертификат.
- Цифровая подпись центра сертификации.
- Связанные поддомены.
- Дата выдачи сертификата.
- Срок действия сертификата.
- Открытый ключ (закрытый ключ не раскрывается).

Зачем нужен SSL-сертификат

SSL-сертификаты сайтов требуются для обеспечения безопасности данных пользователей, подтверждения прав собственности на сайт, предотвращения создание поддельной версии сайта злоумышленниками и обеспечения доверия со стороны пользователей.

Если использование веб-сайта предполагает вход в систему, ввод личных данных, таких как номера кредитных карт, или просмотр конфиденциальной информации, такой как данные медицинской страховки, или финансовой информации, то важно сохранить конфиденциальность этих данных. SSL-сертификаты помогают сохранить конфиденциальность онлайн-транзакций и гарантируют пользователям, что веб-сайт является подлинным и безопасным для ввода личных данных.

Для бизнеса более актуален тот факт, что SSL-сертификаты требуются для веб-адресов HTTPS. HTTPS – это безопасная форма HTTP, то есть трафик веб-сайтов HTTPS зашифрован с помощью SSL. Большинство браузеров помечают сайты HTTP, не имеющие SSL-сертификатов, как небезопасные. Это сигнал пользователям о том, что сайт может быть небезопасным, а для компаний это стимул перейти на HTTPS.

SSL-сертификат помогает защитить такую информацию, как:

- Учетные данные для входа в систему.
- Операции по кредитной карте и информацию о банковском счете.
- Личную информацию: полное имя, адрес, дату рождения, номер телефона.
- Юридические документы и контракты.
- Медицинские документы.
- Конфиденциальную информацию.

Типы SSL-сертификатов

Существуют разные типы SSL-сертификатов с разными уровнями проверки. Шесть основных типов:

1. Сертификаты с расширенной проверкой (EV SSL)
2. Сертификаты, подтверждающие организацию (OV SSL)
3. Сертификаты, подтверждающие домен (DV SSL)
4. Wildcard-сертификаты
5. Мультидоменные сертификаты (MDC)
6. Сертификаты унифицированных коммуникаций (UCC)

Сертификаты с расширенной проверкой (EV SSL)

Это самый высокорейтинговый и наиболее дорогой тип SSL-сертификатов. Как правило, он используется для популярных веб-сайтов, которые собирают данные и используют онлайн-платежи. После установки этого SSL-сертификата в адресной строке браузера отображается замок, HTTPS, название и страна компании. Отображение информации о владельце веб-сайта в адресной строке помогает отличить сайт от вредоносных. Чтобы настроить сертификат с расширенной проверкой, владелец веб-сайта должен пройти стандартизированный процесс проверки подлинности и подтвердить, что он на законных основаниях имеет исключительные права на домен.

Сертификаты, подтверждающие организацию (OV SSL)

Этот тип SSL-сертификатов имеет такой же уровень доверия, что и сертификаты с расширенной проверкой, поскольку для его получения владелец веб-сайта должен пройти основательную проверку. Для этого типа сертификатов информация о владельце веб-сайта также отображается в адресной строке, что позволяет отличить его от вредоносных сайтов. SSL-сертификаты, подтверждающие организацию, обычно являются вторыми по стоимости (после SSL-сертификатов с расширенной проверкой). Их основная цель – зашифровать конфиденциальные данные пользователей при транзакциях. Коммерческие или общедоступные веб-сайты должны устанавливать сертификаты, подтверждающие организацию, чтобы гарантировать конфиденциальность информации о клиентах.

Сертификаты, подтверждающие домен (DV SSL)

Процесс проверки для получения SSL-сертификата этого типа минимален. В результате SSL-сертификаты, подтверждающие домен, обеспечивают меньшую надежность и минимальный уровень шифрования. Такие сертификаты, как правило, используются для блогов или информационных веб-сайтов, т. е. для сайтов, не связанных со сбором данных или онлайн-платежами. Этот тип SSL-сертификатов является одним из самых дешевых и самых быстрых для получения. Процесс проверки требует только, чтобы владелец веб-сайта подтвердил право собственности на домен, ответив на электронное письмо или телефонный звонок. В адресной строке браузера отображается только HTTPS и замок без названия компании.

Wildcard-сертификаты

Wildcard-сертификаты (сертификаты с подстановочными символами) позволяют защитить базовый домен и неограниченное количество поддоменов с помощью одного сертификата. Если имеется несколько поддоменов, которые нужно защитить, приобретение Wildcard-сертификата будет намного дешевле, чем приобретение отдельных SSL-сертификатов для каждого поддомена. Wildcard-сертификаты содержат звездочку (*) как часть общего имени. Звездочка указывается вместо любого допустимого поддомена в составе одного базового домена. Например, один Wildcard-сертификат для веб-сайта можно использовать для защиты следующих страниц:

- payments.yourdomain.com
- login.yourdomain.com
- mail.yourdomain.com
- download.yourdomain.com
- anything.yourdomain.com

Мультидоменные сертификаты (MDC)

Мультидоменные сертификаты можно использовать для защиты нескольких доменных и поддоменных имен, включая сочетания полностью уникальных доменов и поддоменов с разными доменами верхнего уровня (TLD), за исключением локальных / внутренних доменов.

Например:

- example.com
- org
- this-domain.net
- anything.com.au
- example.com
- example.org

По умолчанию мультидоменные сертификаты не поддерживают поддомены. Если требуется защитить сайты www.example.com и example.com с помощью одного

мультидоменного сертификата, то при получении сертификата следует указать оба имени хоста.

Сертификаты унифицированных коммуникаций (UCC)

Сертификаты унифицированных коммуникаций (UCC) также считаются мультидоменными SSL-сертификатами. Сертификаты унифицированных коммуникаций изначально были разработаны для защиты серверов Microsoft Exchange и Live Communications. Сегодня любой владелец веб-сайта может использовать эти сертификаты, чтобы обеспечить защиту нескольких доменных имен с помощью одного сертификата. Сертификаты унифицированных коммуникаций проверяются на уровне организации. Для них в браузере отображается значок замка. Сертификаты унифицированных коммуникаций можно использовать в качестве сертификатов с расширенной проверкой, чтобы обеспечить посетителям веб-сайта максимальную безопасность.

Важно различать типы SSL-сертификатов, чтобы получить правильный тип сертификата для веб-сайта.

Задание.

Составьте по материалам лекции 15 - 20 вопросов с ответами

Как получить SSL-сертификат

SSL-сертификат можно получить непосредственно в центре сертификации. Центры сертификации, иногда также называемые сертифицирующими организациями, ежегодно выдают миллионы SSL-сертификатов. Они играют важную роль в работе интернета и обеспечивают прозрачное и надежное взаимодействие в сети.

Стоимость SSL-сертификата может доходить до сотен долларов, в зависимости от требуемого уровня безопасности. После выбора типа сертификата можно найти издателей сертификатов, предлагающих SSL-сертификаты нужного уровня.

Получение SSL-сертификата включает следующие шаги:

- Подготовка. Настройте сервер, и убедитесь, что ваша запись WHOIS обновлена и соответствует данным, отправляемым в центр сертификации (она должна отображать правильное название и адрес компании и т. д.).
- Создание запроса на подпись SSL-сертификата (CSR) на вашем сервере. С этим действием может помочь ваша хостинговая компания.
- Отправка запроса в центр сертификации для проверки данных о вашем домене и компании.
- Установка полученного сертификата после завершения процесса.

После получения сертификата его необходимо настроить на вашем веб-хосте или серверах, если вы обеспечиваете хостинг веб-сайта самостоятельно.

Скорость получения сертификата зависит от типа сертификата и поставщика сертификатов. Для завершения каждого уровня проверки требуется разное время. Простой SSL-сертификат, подтверждающий домен, может быть выпущен в течение нескольких минут после заказа, а получение сертификата с расширенной проверкой может занять целую неделю.

Можно ли использовать SSL-сертификат на нескольких серверах?

Один SSL-сертификат можно использовать для нескольких доменов на одном сервере. В зависимости от поставщика, можно также использовать один SSL-сертификат на нескольких серверах. Это позволяют мультидоменные SSL-сертификаты, описанные выше.

Как следует из названия, мультидоменные SSL-сертификаты работают с несколькими доменами. Количество доменов остается на усмотрение конкретного центра сертификации. Мультидоменный SSL-сертификат отличается от однодоменного SSL-сертификата, который, как следует из названия, предназначен для защиты одного домена.

Мультидоменные SSL-сертификаты также называются SAN-сертификатами. SAN означает альтернативное имя субъекта. Каждый мультидоменный сертификат имеет дополнительные поля (например, альтернативные имена субъектов), которые можно использовать для перечисления дополнительных доменов, чтобы на них распространялся один сертификат.

Сертификаты унифицированных коммуникаций (UCC) и Wildcard-сертификаты также можно применять на нескольких доменах и, в последнем случае, на неограниченном количестве поддоменов.

Что происходит по истечении срока действия SSL-сертификата?

Срок действия SSL-сертификатов истекает, он не длится вечно. Центр сертификации / Форум браузеров, который де-факто выступает в качестве регулирующего органа для индустрии SSL, заявляет, что срок действия SSL-сертификатов не должен превышать 27 месяцев. По сути, это означает, что SSL-сертификат можно использовать в течение двух лет, плюс до трех месяцев на продление срока действия предыдущего сертификата.

Срок действия SSL-сертификатов истекает, поскольку, как и при любой другой форме аутентификации, информацию необходимо периодически перепроверять и убеждаться в ее актуальности. В интернете все очень быстро меняется, покупаются и продаются компании и веб-сайты. При смене владельцев также меняется информация, относящаяся к SSL-сертификатам. Ограниченный срок действия SSL-сертификатов обеспечивает актуальность и точность информации, используемой для аутентификации серверов и организаций.

Раньше SSL-сертификаты могли выдаваться на срок до пяти лет, который впоследствии был сокращен до трех лет, а в последнее время до двух лет плюс возможность использовать дополнительные три месяца. В 2020 году Google, Apple и Mozilla объявили, что будут применять годовые SSL-сертификаты, несмотря на то, что это предложение было отклонено Центрами сертификации / Форумом браузеров. Это решение вступило в силу в сентябре 2020 года. Не исключено, что в будущем срок действия SSL-сертификатов сократится еще.

Когда срок действия SSL-сертификата истекает, соответствующий сайт становится недоступным. Когда пользователь открывает веб-сайт в браузере, в течение нескольких миллисекунд проверяется действительность SSL-сертификата (в рамках подтверждения SSL-соединения). Если срок действия SSL-сертификата истек, посетители сайта получат сообщение: «Этот сайт небезопасен. Существуют возможные риски».

У пользователей есть возможность продолжить, однако не рекомендуется делать это, учитывая связанные риски кибербезопасности, в том числе вероятность

столкнуться с вредоносными программами. Это существенно влияет на показатель отказов при посещении веб-сайта, поскольку пользователи быстро покидают его.

Осведомленность о сроке истечения SSL-сертификатов является проблемой для крупных предприятий. В то время как малые и средние предприятия имеют один или несколько SSL-сертификатов, крупные предприятия, работающие на различных рынках и имеющие множество веб-сайтов и сетей, имеют также множество SSL-сертификатов. Поэтому причиной того, что компания допустила истечение срока действия своего SSL-сертификата, обычно является недосмотр, а не отсутствие компетентности. Лучший способ для крупных компаний поддерживать осведомленность об истечении срока действия SSL-сертификатов – использовать платформу управления сертификатами. На рынке представлены различные продукты, которые можно найти с помощью онлайн-поиска. Это позволит компаниям просматривать цифровые сертификаты и управлять ими в рамках всей инфраструктуры. При использовании такой платформы важно регулярно входить в систему и проверять, когда необходимо продлить обновления.

Если срок действия сертификата истечет, сертификат станет недействительным, и выполнять безопасные транзакции на веб-сайте станет невозможно. Центр сертификации предложит обновить SSL-сертификат до истечения срока его действия.

Все центры сертификации и службы SSL, используемые для получения SSL-сертификатов, отправляют уведомления об истечении срока действия сертификата с заданной периодичностью, обычно начиная с 90 дней до окончания срока действия сертификата. Постарайтесь, чтобы эти уведомления отправлялись на несколько адресов электронной почты, а не одному человеку, который к моменту отправки уведомления может покинуть компанию или перейти на другую должность. Убедитесь, что соответствующие сотрудники компании включены в список рассылки и своевременно получат уведомление.

Как узнать, есть ли у сайта SSL-сертификат

Самый простой способ узнать, есть ли у сайта SSL-сертификат – обратить внимание на следующие элементы в адресной строке браузера:

- Если веб-адрес начинается с HTTPS, а не с HTTP, значит он защищен с помощью SSL-сертификата.
- Для защищенных сайтов отображается значок закрытого замка, который можно щелкнуть и посмотреть сведения о безопасности. У самых надежных сайтов будут зеленые замки или адресные строки.
- Браузеры также показывают предупреждения, если соединение небезопасно, например красный замок, открытый замок, линию, пересекающую адрес веб-сайта, треугольник-предупреждение над значком замка.

Как обеспечить безопасность онлайн-сеанса

Личные данные и платежные реквизиты можно указывать только на веб-сайтах, защищенных сертификатами с расширенной проверкой или сертификатами, подтверждающие организацию. Сертификаты, подтверждающие домен, не подходят для сайтов электронной коммерции. Сайты, защищенные сертификатами с расширенной проверкой или сертификатами, подтверждающими организацию, можно определить, посмотрев на адресную строку. Для сайтов, защищенных сертификатами с расширенной проверкой, название организации отображается в адресной строке. Для сайтов, защищенных сертификатами, подтверждающими организацию, данные о

названии организации, отображаются по щелчку на значке замка. Для сайтов с сертификатами, подтверждающими домен, отображается только значок замка.

Ознакомьтесь с политикой конфиденциальности веб-сайта. Это позволяет понять, как будут использоваться ваши данные. Законопослушные компании обычно прозрачно описывают сбор и действия с данными.

Обратите внимание на сигналы и индикаторы, вызывающие доверие к веб-сайту.

Наряду с SSL-сертификатами, это могут быть логотипы или значки, показывающие репутацию и соответствие веб-сайта определенным стандартам безопасности. Другие признаки, по которым можно оценить сайт, включают проверку физического адреса и номера телефона, ознакомление с политикой возврата товаров и средств, проверку правдоподобности цен – ведь бесплатный сыр может оказаться в мышеловке.

Будьте внимательны к фишинговым атакам.

Иногда злоумышленники создают веб-сайты, имитирующие существующие, чтобы обманом заставить людей сделать покупку или выполнить вход на фишинговый сайт. Фишинговый сайт может получить SSL-сертификат и, следовательно, зашифровать весь трафик, проходящий между сайтом и пользователями. Растущая доля фишинговых атак происходит на HTTPS-сайтах. Происходит обман пользователей, которых успокаивает наличие значка замка.

Чтобы избежать подобных атак:

- Всегда проверяйте, что домен сайта, на котором вы находитесь, написан правильно. Веб-адрес поддельного сайта может отличаться только одним символом, например, amaz0n.com вместо amazon.com. В случае сомнений введите домен прямо в браузере, чтобы убедиться, что вы подключаетесь именно к тому веб-сайту, который собираетесь посетить.
- Никогда не вводите логины, пароли, банковские реквизиты и другую личную информацию на сайте, если вы не уверены в его подлинности.
- Всегда оценивайте, что предлагается на сайте, не выглядит ли он подозрительным и действительно ли вам нужно на нем регистрироваться.
- Убедитесь, что ваши устройства защищены надлежащим образом: Kaspersky Internet Security проверяет веб-адреса по базе фишинговых сайтов и обнаруживает мошенничество независимо от того, насколько безопасным выглядит ресурс.

Угрозы кибербезопасности продолжают расти, но понимание типов SSL-сертификатов, и того, как отличить безопасный сайт от потенциально опасного, поможет интернет-пользователям избежать мошенничества и защитить свои личные данные от киберпреступников.

Задание 2.

Создайте презентацию по материалам лекции